



Micro Leasing Public Company Limited

Enterprise Risk Management Policy

Table of Contents

	Page
1. Objectives	1
2. Risk Management Structure	1
3. Company's Main Risk Management Approach	4
4. Risk Matrix and Risk Management Framework	5
5. Review of Corporate Risk Management Policy	9

Enterprise Risk Management Policy

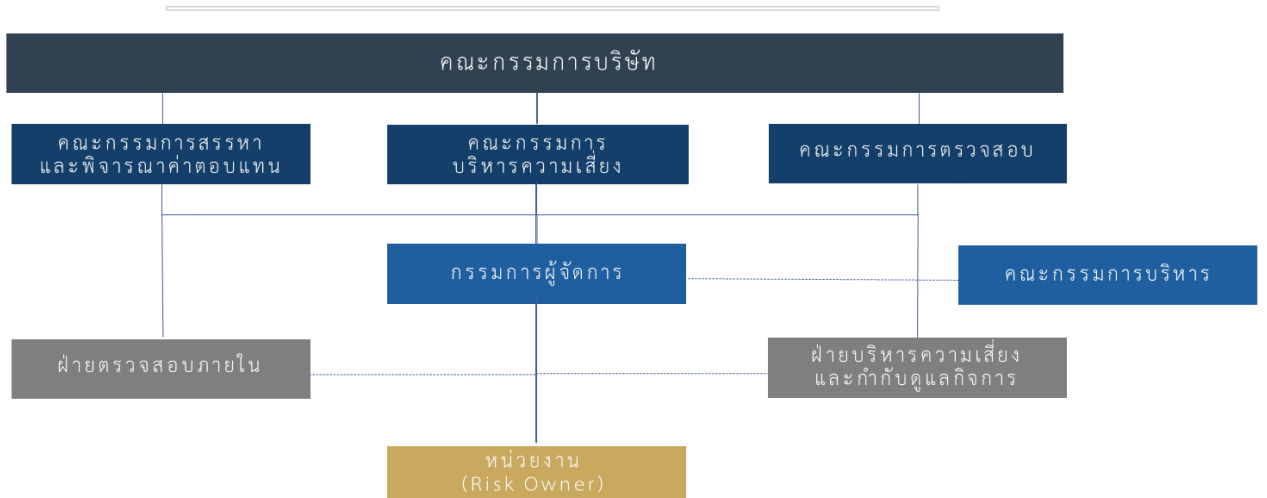
1. Objectives

The objective of the corporate risk management framework is to provide the company with an effective approach to managing corporate risks, enabling the organization to achieve its operational goals within an appropriate and acceptable risk framework. This leads to value creation for the organization and its stakeholders. The company adopts risk management guidelines from the Committee to Sponsoring Organizations of the Treadway Commission (COSO), the regulations of the Stock Exchange of Thailand, the practices of the Bank of Thailand, and other relevant official rules and laws. These guidelines are used to formulate corporate risk management policies and strategies, which are regularly reviewed for appropriateness and adequacy to align with the business environment. The company continuously develops its corporate risk management system to ensure effective risk management in accordance with international standards, covering five key risk areas: strategic risk, credit risk, liquidity risk, market risk, and operational risk, including information technology risk and reputational risk.

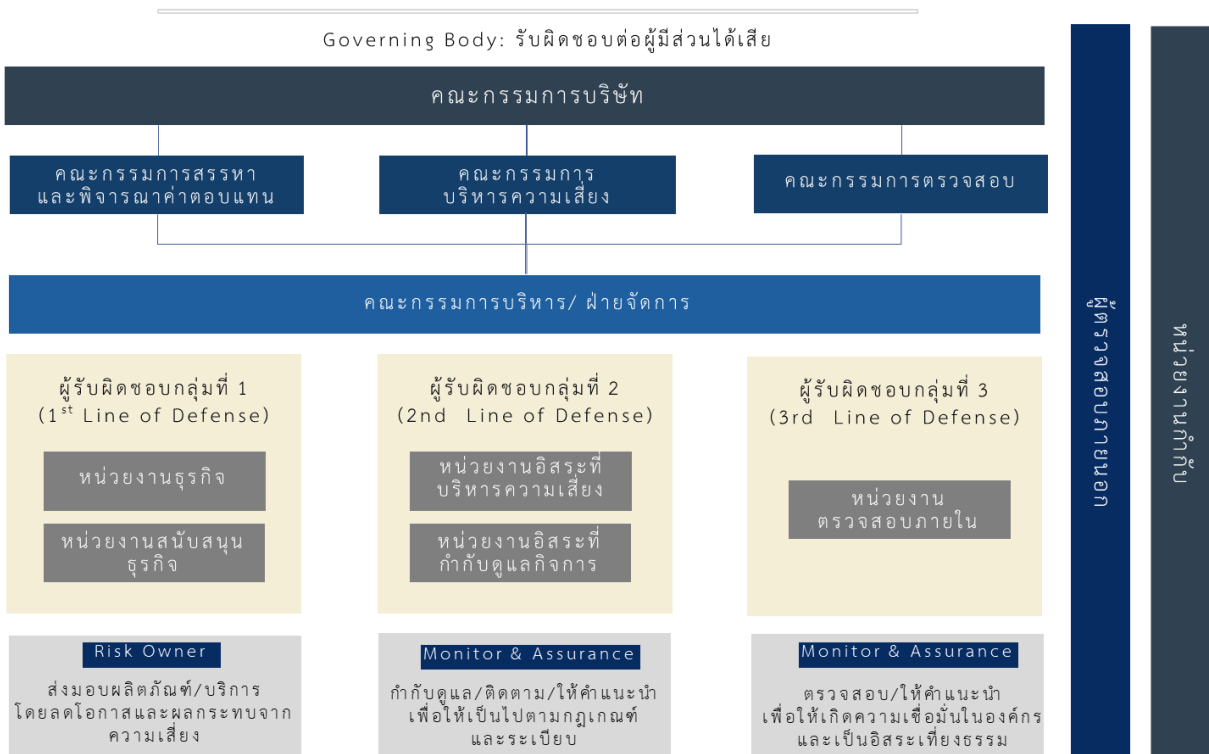
2. Risk Management Structure

Risk management is an integral part of all business processes and is interconnected at all levels. Therefore, the risk management structure must be cohesive. The Risk Management Committee sets policies, drives, and monitors risk management, while each unit is responsible for assessing and managing risks according to their respective responsibilities. The risk management structure includes:

โครงสร้างการบริหารความเสี่ยง



โครงสร้างและบทบาทของผู้รับผิดชอบตามหลัก Three Line of Defense



Overall Risk Management Structure, the company's risk management responsibilities are divided into three levels: the Board level, the Management level, and the Operational level. The Board level includes the Board of Directors, the Risk Management Committee, the Audit Committee, the Nomination and Remuneration Committee, the Executive Committee, and the Management. The Management level acts as the Governing Body, responsible to the company's stakeholders. It establishes the structure and roles of those responsible according to the Three Lines of Defense principle at the operational or departmental level to ensure checks and balances within the internal control framework, supporting various risk management activities. The Operational level is divided into three lines of defense as follows:

- 1. First Line of Defense:** This consists of the Risk Owners or operational units that directly face risks in their operations. They are responsible for overseeing their own work to comply with official regulations, company policies, and procedures, and to implement appropriate internal controls and risk management to reduce the likelihood and impact of various risks.
- 2. Second Line of Defense:** This includes independent units responsible for setting policy frameworks, regulations, standards, and risk management processes. They oversee the operations of units to ensure compliance with official regulations, company policies, and procedures, and support units in managing risks appropriately. They also provide advice, knowledge transfer, communication, and monitoring of various units' practices. This includes the Risk Management and Corporate Governance Department, which reports directly to the Risk Management Committee.
- 3. Third Line of Defense:** This includes independent units responsible for auditing risk management processes and methods, reviewing and evaluating the effectiveness of risk management processes of the first and second lines of defense, and providing recommendations to improve risk management and internal controls to better reflect the actual operations of the units. This includes Internal Audit, which reports directly to the Audit Committee.

The corporate risk management policy covers overall risk management for the company and its business group to ensure that overall risk management follows a standardized approach across the business group.

3. Company's Main Risk Management Approach

The company employs an integrated corporate risk management approach, aligning risk management with the company's strategic plans, planning, and investments. The main risk management approach covers five key risk areas: strategic risk, credit risk, liquidity risk, market risk and operational risk, including information technology risk, compliance risk, and reputational risk.

3.1 Strategic Risk Management

Strategic risk refers to the risk arising from inappropriate strategic planning and execution, as well as inconsistencies between policies, strategic goals, organizational structure, competitive conditions, resources, and the environment, which affect the organization's objectives or goals.

The company continuously develops and improves strategic risk management according to COSO guidelines by creating corporate risk management plans. The company also regularly reviews its policies and strategic plans, considering risk factors that may impact the company's strategic plans to ensure an adequate and effective strategic risk management process that supports and controls strategic risks within acceptable levels.

3.2 Credit Risk Management

Credit risk refers to the risk that debtors or counterparties of the company may not fulfill their contractual obligations related to lending, investment, and commitments, such as debtors failing to repay principal or interest as agreed with the company.

The company establishes an adequate credit risk management process, including managing credit portfolio risks from credit concentration and counterparty credit risks, to effectively support and control credit risks. This includes credit assessment and approval, provisioning for asset impairment, and monitoring debt quality, using tools and statistical data to determine risk-adjusted returns and conduct stress testing to assess the impact of internal and external factors on credit quality and financial position, ensuring adequate capital management.

3.3 Operational Risk Management

Operational risk refers to the risk arising from all operational processes due to poor governance or inadequate internal controls, covering factors related to processes, equipment, information technology, personnel, and asset security.

The company emphasizes raising awareness and prioritizing business continuity management in a changing environment. It provides knowledge transfer to Risk Owners for self-assessment of risks and internal controls (Risk Control Self-Assessment: RCSA) and key risk indicators (Key Risk Indicator: KRI), as well as reporting operational losses (Loss Data) and incidents causing damage (Incident). Operational risk management also covers information technology risk, compliance risk, and reputational risk.

3.4 Liquidity Risk Management

Liquidity risk refers to the risk that the company may not meet its obligations when due because it cannot convert existing assets into cash or cannot obtain sufficient funds to meet cash flow needs within the specified time and at an appropriate cost, potentially causing damage.

The company closely monitors liquidity risk levels and events that may directly or indirectly impact liquidity risk. Additionally, the company continuously and regularly assesses and analyzes liquidity risks to ensure sufficient liquidity for business operations, such as evaluating capital inflows and outflows, forecasting future liquidity positions, and using various liquidity ratio.

3.5 Market Risk Management

Market risk refers to the risk that the company may incur losses due to changes in the value of the company's financial position reported in the balance sheet, resulting from movements or volatility in interest rates, securities prices, and exchange rates.

The company has a market risk management process to mitigate potential losses to income and/or the company's economic value by setting policies and risk limits, as well as monitoring and controlling market risks, such as managing net interest income margins and aligning interest income and expense structures.

4. Risk Matrix and Risk Management Framework

All units must regularly report their risk management results to the Risk Management and Corporate Governance Department, which consolidates and reports to the Risk Management Committee for further consideration. Risk assessments must cover the Risk Matrix and risk management framework as defined by the company.

4.1 Risk Matrix

All Risk Owners must analyze, assess, and rank risks, and prepare appropriate risk management measures or approaches. The assessment considers two dimensions:

- 1) **Likelihood or Frequency:** To evaluate the probability of risk events occurring.
- 2) **Severity or Impact:** To assess the level of impact from inherent risk and residual risk, as well as other risks, if risk events occur.

The risk level is calculated as the product of (1) the likelihood of the risk occurring and (2) the severity of the impact. The risk assessment levels (Risk Scale) are defined according to the Risk Matrix as follows:

Severity/ Impact							
5	Intolerable	5	10	15	20	25	
4	Undesirable	4	8	12	16	20	
3	Tolerable	3	6	9	12	15	
2	Acceptable	2	4	6	8	10	
1	Insignificant	1	2	3	4	5	
		Rare	Unlikely	Possible	Likely	Almost Certain	
		1	2	3	4	5	Likelihood

VH	Very High >> ระดับความเสียหายสูงมาก - คะแนนระดับความเสียหาย 17-25 คะแนน
H	High >> ระดับความเสียหายสูง - คะแนนระดับความเสียหาย 10-16 คะแนน
M	Medium >> ระดับความเสียหายปานกลาง - คะแนนระดับความเสียหาย 5-9 คะแนน
L	Low >> ระดับความเสียหายต่ำ - คะแนนระดับความเสียหาย 3-4 คะแนน
VL	Very Low >> ระดับความเสียหายต่ำมาก - คะแนนระดับความเสียหาย 1-2 คะแนน

4.2 Risk Response and Risk Mitigation

All Risk Owners must establish risk management approaches and/or risk prevention strategies and/or appropriate controls measures to respond to potential risks. These measures aim to reduce likelihood and impact of potential adverse effects. Additionally, they must develop action plans to be implemented. The risk response and mitigation approaches include:

การตอบสนองความเสี่ยง (Risk Response)					
Probability/ Likelihood	Severity/ Impact				
	Insignificant	Acceptable	Tolerable	Undesirable	Intolerable
Almost Certain	TA/ TR/ TS	TA/ TR/ TS	TA/ TR/ TS	TA/ TR/ TS/ AT	TA/ TR/ TS/ AT
Likely	TA/ TR	TA/ TR/ TS	TA/ TR/ TS	TA/ TR/ TS	TA/ TR/ TS/ AT
Possible	TA/ TR	TA/ TR/ TS	TA/ TR/ TS	TA/ TR/ TS	TA/ TR/ TS
Unlikely	TA	TA/ TR	TA/ TR/ TS	TA/ TR/ TS	TA/ TR/ TS
Rare	TA	TA	TA/ TR	TA/ TR	TA/ TR/ TS

Risk Response

การยอมรับ	TA	Take/Accept: ความเสี่ยงอยู่ในระดับที่ยอมรับได้ ยังคงใช้วิธีการเดิมที่อยู่ได้ หรือบริหารจัดการความเสี่ยงโดยการลด แบ่ง/ถ่ายโอน หรือหลีกเลี่ยง ก็ได้ เช่น การกำหนดงบประมาณรองรับเหตุการณ์/ ความสูญเสีย การดูแลติดตามความเสี่ยงอย่างสม่ำเสมอ การกำหนดแผนสำรองกรณีฉุกเฉิน
การควบคุม/ลด	TR	การควบคุม/ลด TR Control/ Treat/Reduce: ความเสี่ยงอยู่ในระดับที่ต้องจัดการ ควบคุม หรือลด โดยจัดหาวิธีการจัดการเพิ่มเติม เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ เช่น การกำหนดกรอบอำนาจอนุมัติ การระบอบยอด การแบ่งแยกหน้าที่
การถ่ายโอน/แบ่งเบา	TS	Transfer/Share: ความเสี่ยงอยู่ในระดับที่ต้องถ่ายโอน หรือแบ่งเบาความเสี่ยง โดยจัดหาผู้รับผิดชอบร่วม เช่น การทำประกันภัย การร่วมทุนหรือคู่ค้า การทำ Hedging การใช้ Outsource การกระจายหุ้น
การหลีกเลี่ยง	AT	Avoid/Terminate: ความเสี่ยงอยู่ในระดับที่องค์กรไม่สามารถยอมรับได้ จัดการโดยหยุดโครงการ ธุรกิจ หรืองานที่มีความเสี่ยงนั้น หรืออาจปรับลดความเสี่ยงโดยการถ่ายโอน หรือแบ่งเบาความเสี่ยง เช่น การหยุดกิจกรรมธุรกิจ/ ธุรกิจ การออกจากตลาด การลดสัดส่วนการลงทุน การปรับแผนกลยุทธ์ การปรับปรุงกระบวนการใหม่

The selection of risk management approaches must be appropriate for the level of residual risk, considering the cost-to-benefit ratio to ensure the company gains the maximum benefit.

4.3 Levels of Likelihood/Frequency and Severity/Impact

All Risk Owners must assess risks based on the framework of likelihood and frequency of risk occurrence (Likelihood/Frequency) and the severity of impact and nature of damage (Severity/Impact). The definitions and details are provided in the following table:

คะแนน Score	ระดับความเสี่ยง Risk Level	ลักษณะโอกาส หรือความถี่ที่เกิดความเสี่ยง(Likelihood/Frequency)			ระดับความรุนแรงของผลกระทบ / ลักษณะของความเสียหาย(Severity/Impact)				
		เหตุการณ์ Event	โอกาสเกิด Probability	ความถี่ Frequency	ค่าความเสียหาย/ Financial Loss	ด้านกฎหมาย/ การปฏิบัติงาน/กฎระเบียบของบริษัท	ด้านลูกค้า/ภาพลักษณ์ของบริษัท	ด้านความปลอดภัย	
1	Low	เป็นเหตุการณ์ที่คาดว่าจะมีโอกาสที่จะเกิดขึ้นในขนาดน้อยมาก	น้อยมาก Rare	≤ 2%	กระบวนการ หรือธุรกรรมนั้นเกิดขึ้นในรอบระยะเวลาตั้งแต่ 1 ปี ขึ้นไป (Yearly)	≤ 10,000 บาท	แทบไม่มีผลกระทบต่อกรปฏิบัติงาน	ไม่กระทบกับลูกค้า/ไม่กระทบชื่อเสียงของบริษัท	อันตรายต่อร่างกาย ขึ้นปฐมพยาบาลเองได้
2	Rather low	เป็นเหตุการณ์ที่คาดว่าจะมีโอกาสที่จะเกิดขึ้นในขนาดน้อย	น้อย Unlikely	> 2 – 5%	กระบวนการ หรือธุรกรรมนั้นเกิดขึ้นในรอบระยะเวลาตั้งแต่ 6 เดือน แต่ไม่ถึง 1 ปี (Half-Year)	มากกว่า 10,000 - 50,000 บาท	มีผลต่อการปฏิบัติงานที่ไม่มีนัยสำคัญ/ ไม่กระทบรายได้ของบริษัท/ ได้รับการดักเตือนหรือคิดเบี่ยงปรับที่มูลค่าไม่มีนัยสำคัญ	กระทบลูกค้าจำนวนน้อย / ชื่อเสียงเสียหายจำกัดอยู่ในวงเฉพาะ / ปรากฏข่าวลือที่อาจพาดพิงคนภายในบริษัท	อันตรายต่อร่างกาย เข้ารักษาใน ร.พ. และหยุดงาน 1-5 วัน
3	Medium	เป็นเหตุการณ์ที่คาดว่าจะมีโอกาสที่จะเกิดขึ้นในขนาดปานกลาง	ปานกลาง Possible	> 5-10 %	กระบวนการ หรือธุรกรรมนั้นเกิดขึ้นในรอบระยะเวลาตั้งแต่ 3 เดือน แต่ไม่ถึง 6 เดือน (Quarterly)	มากกว่า 50,000 - 100,000 บาท	มีผลต่อการปฏิบัติงาน/ กระทบรายได้ของบริษัท / ตอบชี้แจงหรือส่งหลักฐานต่อทางการ และถูกคิดเบี่ยงปรับแต่ยังคงอยู่ในเกณฑ์ที่รับได้	กระทบลูกค้าจำนวนปานกลาง/ บางส่วนไม่พอใจการให้บริการของบริษัท แต่ยังไม่ทำธุรกิจกับบริษัท/ ชื่อเสียงถูกเผยแพร่แต่ไม่มีผลสะท้อนกลับ	อันตรายต่อร่างกาย ขึ้นมาดเจ็บเข้ารักษาใน ร.พ. และหยุดงานมากกว่า 5 วัน
4	Rather high	เป็นเหตุการณ์ที่คาดว่าจะมีโอกาสที่จะเกิดขึ้นในขนาดสูง	สูง Likely	> 10 – 20%	กระบวนการ หรือธุรกรรมนั้นเกิดขึ้นในรอบระยะเวลาตั้งแต่ในรอบสัปดาห์ แต่ไม่ถึง 3 เดือน (Weekly/ Monthly)	มากกว่า 100,000 - 200,000 บาท	มีผลต่อการปฏิบัติงาน และการดำเนินธุรกิจของบริษัทมาก / ถูกทางการตรวจสอบและชี้มูลความผิด และถูกคิดเบี่ยงปรับที่มูลค่ามีนัยสำคัญ	กระทบกับลูกค้าจำนวนมาก/ บางส่วนไม่พอใจและยกเลิกการใช้บริการกับบริษัทบ้าง / ชื่อเสียงถูกเผยแพร่ออกไปพอสมควร / สื่อสังคมออนไลน์เผยแพร่ข่าวด้านลบของบริษัท	อันตรายต่อร่างกาย ขึ้นมาดเจ็บสาหัส
5	High	เป็นเหตุการณ์ที่คาดว่าจะมีโอกาสที่จะเกิดขึ้นในขนาดสูงมาก	สูงมาก Almost Certain	> 20%	กระบวนการ หรือธุรกรรมนั้นเกิดขึ้นในทุกวัน (Daily/ Many times per day)	มากกว่า 200,000 บาทขึ้นไป	มีผลต่อการดำเนินธุรกิจและรายได้ของบริษัทเป็นอย่างมาก/ ถูกยกเลิกสัญญา/ ใบอนุญาต/ กรรมการและผู้บริหารระดับสูงของบริษัท อาจถูกลงโทษตามกฎหมาย	กระทบกับลูกค้าจำนวนมาก ส่งผลต่อการดำเนินธุรกิจ/ ลูกค้ายกเลิกการใช้บริการของบริษัท/ ชื่อเสียงเสียหายไปทั่วประเทศ	อันตรายต่อร่างกาย ขึ้นสูญเสียชีวิต

5. Review of Corporate Risk Management Policy

The company mandates a review of the corporate risk management policy whenever events occur that may significantly impact the achievement of corporate risk management objectives, or at least once a year. This is to ensure that the policy is updated to reflect changing conditions that may significantly affect corporate risk management. The Risk Management and Corporate Governance Department is responsible for this review and will present it to the Risk Management Committee for approval before submitting it to the Board of Directors for final approval.